DataKeep™

SecurityFirst™ Protecting Critical Data

Integrated and Transparent Key Management with DataKeep™

Overview

The algorithm described by the Advanced Encryption Standard (AES) is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data. It is the first (and only) publicly accessible cipher approved by the National Security Agency (NSA) for top secret information when used in an NSA approved cryptographic module. By protecting data using AES-256, a cybercriminal using a brute force attack will need to generate 2256 different key combinations to break an encrypted message; a feat which is virtually impossible using even the fastest available computers.

What follows is a description of how SecurityFirst's DataKeep™ technology performs key management functions.

Key Structure

1. The strength of all DataKeep keys is symmetric 256 bits, with each being randomly generated via a certified, random key generation module. The technology uses a transparent approach to key generation and data protection including three possible layers depending upon the chosen deployment model:DataKeep agents create up to three file- or volume-based Data Encryption Keys (DEK). A volume agent will use a single set of keys for all data within the defined volume or partition, whereas a file agent will create a unique set of keys for each directory specified in an associated policy. DEK's include:

a. The 256-bit encryption key used by AES-256 standard.
b. The Splitting Key used by the bit splitting operation.
c. The Authentication Key (used by GMAC or HMAC as applicable) which provides assurance that the resulting split data has not been tampered with or corrupted prior to use (not available in the 1:1 data construct).
2. The Policy Encryption Key (PEK) is used to determine policy enforcement, as well as protect the underlying key structure as the key encryption key via wrapping the volume and file DEKs.

3. The Key Wrapping Key (KWK) is an externally generated and stored encryption key used whenever an external hardware key store is specified. It encrypts the PEKs. and allows the customer to both specify and control this highest-level key.

This layered approach provides several benefits in key management, access control, and data protection including:

- The PEK secures the data behind the operational permission enforcement based on OS user/group definitions.
- The PEK, when used in conjunction with a file-based agent, can additionally provide cryptographic separation of data within the context of a policy for isolation of data, or across policies where customers have defined a community of interest with shared access.
- The PEK is also the core of key rotation and revocation operations as noted in key management (below).

With all keys contained in secure environments, no external hardware key store is required except as needed for corporate or regulatory requirements. In that case, Key Management Interoperability Protocol (KMIP) is supported for the external key store and protect the KWK.

Key Storage and Access

Within DataKeep, keys are stored in two locations for internal use and protection. Firstly, because the PEK is aligned with policy and access controls, it is stored in the Policy, Provisioning, and Management (PPM) database. As required, PEKs are transmitted securely to each agent, but they do not persist. A system reboot will require the agent to reconnect to an authorized PPM to authenticate and receive the policy table containing the PEKs aligned with specifications. Secondly, the file-based keys are stored in the header of the volume or file respectively dependent on the agent type.

Remote via KMIP: When an optional KMIP compatible external key store is configured, the PPM supports the KMIP standard. In this case, the external device is used as a key store to replace the internal key store.

Hardware Keystore: When a hardware key store is used, an externally generated and managed key (the KWK) is used to wrap the PEKs before they are stored in the PPM database.

All management of the PEKs (i.e. creation, rotation, revocation, or retrieval for agent bring up) is done by the PPM.

Key Management

For key generation, DataKeep uses two instances of its certified key generation module: one in the PPM for PEKs, and one in the agent for DEKs--both volume- and file-based. Each instance relies on random system heuristics and FIPS-certified algorithms to generate symmetric 256 bit keys for each of the protection steps.

Key rotation operations are acted upon at the PEK layer where access controls are enforced. As a result, only the PEK is quickly rotated using just the header while keeping the data encrypted throughout the process.

Key shredding is similar to key rotation, but deletes the key in PPM and forces a reboot of the agent. The policy at the agent level has no context to allow access or decryption of the data associated with one or more PEKs effectively crypto-shredding the data.

DataKeep – The Solution

DataKeep is the next generation of truly secure data-centric protection for organizations looking to protect their digital assets. By implementing the DataKeep solution, organizations can mitigate risk associated with unauthorized access to data, gain business and cost efficiencies, garner complete control of data at all times, and employ a protect everything security strategy and alleviate the burdens associated with identifying sensitive data.

A single management console is used to administer all data access policies and provisions lightweight encryption agents to servers where data needs to be protected. DataKeep supports the separation of duties between security and product administrators, and privileged access management prevents root access and cloud service providers from seeing unencrypted data.

DataKeep helps assure data privacy and protects against brute force attacks. The SPxCore™ technology combines AES-256 certified encryption and internal key management certified by the National Institute of Standards and Technology (NIST) to be FIPS 140-2 compliant. For your added protection, no “backdoor” exists, even for intelligence or law enforcement agencies. For deployment flexibility, DataKeep works at both the storage volume and individual file levels.

All event logging (permits and denies) occurs in real time and is recorded for review or can be forwarded to a security information event monitoring (SIEM) application. DataKeep will help you meet regulatory requirements for DFAR, NIST, HIPAA, HITECH, FISMA, Sarbanes-Oxley, GBLA, PCI and more including most local, state and global requirements.

SecurityFirst™ delivers advanced security solutions that build a firewall around your data to protect against ever increasing threats and to aid in meeting regulatory requirements such as GDPR, HIPAA, NYCRR and many others.

DataKeep™, our flagship product, serves as your data firewall by using advanced encryption, scalable hierarchical key management, extensive policy enforcement and monitoring of unauthorized access to deliver the highest levels of availability, resiliency and time to value. Security requires a layered approach and protection of the data itself is your last line of defense.

SecurityFirst™
Protecting Critical Data

For a product demonstration or more information contact:
sales@securityfirstcorp.com
888-884-7152
securityfirstcorp.com